University of Alberta

Internet Crimes: Can and Should the Internet be Regulated?

by

Lisa D. Clyburn

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Education

Department of Educational Psychology

Edmonton, Alberta

Fall, 1998

National Library of Canada
Acquisitions and Bibliographic Services
395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale du Canada
Acquisitions et services bibliographiques
395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-34449-5

Canada

UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled INTERNET CRIMES: CAN AND SHOULD THE INTERNET BE REGULATED? submitted by Lisa D. Clyburn in partial fulfillment of the requirements for the degree of Master of Education.

Dr. E.W. Romaniuk

Dr. G. Buck

Dr. R. Mulcahy

September 25, 1998
Date

Abstract

The purpose of this study was to explore the growing challenge of Internet crime, including its prevalence, and the feasibility of regulating the Internet. Fifty-two school officials from Alberta school districts, twelve university respondents from various Canadian universities, and members of eleven police departments from across Canada completed surveys on the issue of concern. Descriptive statistics on the numerous questionnaire responses were employed to analyze the data. The findings of the study indicate that most schools and universities which participated in the study used some form of restricted access to the Internet, and enforced policies that they viewed as successful. Internet fraud was viewed as the most prevalent crime by the police departments surveyed and the most frequently investigated Internet crime. The police survey also revealed that most departments did not believe regulation of the Internet is feasible.

Self-regulation is likely the best option to limiting Internet crime. Education and increased awareness of Internet crime can also help. Legislation likely needs to be adapted to meet the increasing challenge of Internet crime. In addition, parents and teachers need to take safeguards towards keeping children safe from the dangers associated with Internet – based crime.

To Nanny C., an eternal Kindred Spirit . I miss you. Until we meet again....

Acknowledgments

Ahhh, it's done. It really is done. It's been a long time coming, so it is with great pleasure that I write this acknowledgment page. Although there were many times this thesis felt like a huge burden (and in 3 different provinces), the satisfaction of its completion has made it worthwhile (okay, maybe that's pushing it)...

In any case, there are a number of people I would like to thank for their support for the duration of the project . Firstly, I would like to thank my supervisor, Dr. Romaniuk, for his patience during each process of the project, especially during my re-locations to Ontario and PEI. Dr. Buck, a committee member, is to be commended for his helpful ideas and feedback, and his never-ending positive reinforcement. I also thank Dr. Mulcahy for serving on my committee, and for his interest in the subject. A hearty thank you also goes out to Det. George Sidor and Det. Dave Johnston for enlightening me on the procedures for battling Internet crimes, and for their contributions to this project.

A very special thank you goes out to my twin sister Leah. Her support and faith in the completion of this thesis was unwavering. Sis, you are truly a blessing, and a best friend.

Heartfelt thanks goes out to my family in Nova Scotia, and my friends (my Alberta family) for their support. I'm sure you are just as glad to see this thesis finished...

Lastly, honorable mention goes out to the person to whom I have dedicated this thesis. Although my precious grandmother is no longer with us here on Earth, she is with us in spirit, and as my guardian angel. She will always hold a special place in my heart,

and although she is not here to see the culmination of my thesis, I know that she would be proud. I love you and miss you, my Angel and Kindred Spirit.

Thank you to all others who have helped in any way, and listened to me ramble during those "stress attacks" (including Yoda). I am forever grateful.

Table of Contents

Content	Page
Chapter 1 - Introduction	1
Cybercrimes	2
Pornography on the Internet	3
Copyright infringements and fraud on the Internet	6
Hate groups and defamation on the Internet	8
Bomb-making information on the Internet	9
Hacking	10
The law	11
Canadian law	11
Communication Decency Act (CDA) of the United States	14
Cyberpatrols	15
Who is responsible?	16
Arguments for and against regulating the Internet	18
Background to Study	21
Summary of gaps in literature	32
Purpose of study	32
Chapter II - Method	34
Subjects	34
School officials	34
University officials	34

Police departments 34
Survey instruments 34
School questionnaire 34
University questionnaire 34
Police questionnaire 35
Procedure 35
Chapter III - Results 38
Police questionnaire 38
University questionnaire 44
School questionnaire 48
Chapter IV - Discussion and Conclusions 56
Summary of findings 57
Police questionnaire 57
University questionnaire 58
School questionnaire 59
Summary 60
Possible solutions to regulation 60
Myths about the accessibility of obscene material 60
Filtering products and warning labels 61
Self-regulation and user responsibility 63
Education of users and the legal community 63
Advice for parents and teachers 64

Limitations of study 65

Recommendations for future research 65

Conclusion 67

References 68

Appendix A - School Questionnaire 72

Appendix B - University Questionnaire 74

Appendix C - Police Questionnaire 76

Appendix D - Universities Used in Study 78

Appendix E - Letter of Explanation 80

Appendix F - Follow-up Letter Sent with All Surveys 81

Appendix G - Police Departments Used in Study 82

Appendix H - List of School Districts Used in Study 84

List of Tables

Table	Description	Page
1	Number and percentages of charges laid in past twelve months due to Internet crimes, as reported by police	40
2	Number and percentages of complaints currently being investigated as reported by police	41
3	Number and percentages of universities reporting restrictions on Internet access	46
4	Number and percentages of universities reporting various procedures for restriction of Internet access	47
5	Number and percentages of schools reporting restrictions on Internet access	50
6	Number and percentages of schools reporting various procedures for restriction of Internet access	54

Chapter 1

Introduction

Internet Crimes: Can and Should the Internet be Regulated?

It has been suggested that by the year 2003, almost every person on earth could be connected to the Internet (Treese, 1997). The Internet has contributed to the vast realm of knowledge available at a person's fingertips. Computers are becoming more widespread and easier to use, partly due to declining costs. In 1994, 25% of Canadian households had a home computer, up from 10% in 1986 (General Social Survey, 1994). One in three of these home computers was equipped with a modem, which is necessary to explore the Internet. The survey also found that in 1994, 56% of adult Canadians (12.3 million) were able to use a computer, up substantially from 47% in 1989. In addition, in 1994, 41% of Canadians aged 15 and over had taken at least one computer course. When asked about Internet services, the General Social Survey (1994) revealed that in 1994, 17% of computer users (2.2 million) reported having used an on-line service or the Internet in the 12 months before the survey (Frank, 1994). The combination of inexpensive computers, and easy access to the Internet means that it can now be enjoyed by persons such as grandparents, business people, students, and children. However, the Internet can also be exploited by many different types of people, as well as serving as a means of exploitation. As more people go on-line, it only seems natural that some form of malice is more likely to occur.

Investigation into the regulation of the Internet has gained attention recently due to an increase in criminal activity that has been ascribed to the Internet. The Internet has

the potential to act as an innocuous venue for those individuals who may feel uncomfortable purchasing sexually explicit materials in a bookstore. "Where an adult or a youngster may be too shy to enter an erotic boutique in the local mall, perusing and ordering products with the privacy of a computer has appeal" (Laughon & Hanson, 1996, p. 18). Computers and the Internet have allowed the masking of persons' identities because some e-mail can be sent anonymously using anonymous re-mailers, they can mingle in chat rooms under aliases, and they can send nasty and false messages to other newsgroups. Often, this is done without repercussions. "The Internet is a breeding ground for all kinds of expression, some of it logical and wise, but some of it vile and hateful, all of it easily accessible to anyone who logs on" (Diamond & Bates, 1995, p. 24).

The present study examines this aspect of the Internet and explores the magnitude of Internet crime in Canada as well as the policies that currently exist to help regulate Internet activity. A greater understanding of this issue and an evaluation of the regulations currently in place are critical in gaining control over this important and growing problem.

Cybercrimes

As exploring the Internet increases in popularity, and accessibility is facilitated, criminal activity is likely to increase. Both the general public and law enforcement officials on and off the Internet will likely need to adjust to the growing concerns. The different types of crimes prevalent on the Internet have been given increasing media attention as they become more popular. Due to its severity and preponderance,

pornography has been featured most frequently in media sources when compared to other cybercrimes.

Pornography on the Internet

Because the Internet can be such a safe haven in which to post obscene material, the Internet can be referred to as the biggest existing porn shop. Particular Internet links quickly introduce pedophiles, who are seeking unsuspecting children to victimize, or salespeople who are promoting their pornographic materials. Anyone who knows how to spell s-e-x and use a search engine can access pornographic sites. A short distance away from these homepages are potential links to images of bestiality, children involved in bondage, or sex with violence. This seemingly ease of access to pornographic material may intrigue some Internet surfers, who test just how easy it is to find and view these pages. Most of the pornographic material, however, appears in files which can be downloaded from easily accessible newsgroups, which are a form of public bulletin board systems. This ease of accessibility is a likely factor contributing to the amount of media attention given to pornographic activities in recent years. Skeptics may argue that the prevalence of the problem is exaggerated due to the attention it receives. Nonetheless, the posting of illegal pornographic material keeps law enforcement officials busy. In September 1998, fourteen countries (including Canada) were involved in the mass arrests of about 200 suspected pedophiles whose homes were raided simultaneously. This type of police action required a great deal of international cooperation. The pornographic pictures exchanged among the pornography ring included those of children as young as two years of age. The charges ranged from possession of pornographic material to sexual

abuse. The variation of charges was due to the different judiciary systems of the involved countries.

Edmonton, Alberta was one of the first Canadian cities to have municipal police officers devoted to the investigation of crime on the Internet. In September 1996 these resources were put to use. Two men were charged for distributing pornographic material via the Internet. Because most of the material in these circumstances is usually sent anonymously to various newsgroups, tracing the perpetrator can pose a real challenge. Newsgroups are a commonly used electronic service; currently there are over 20,000 newsgroups on a vast number of different topics. Internet users can read the messages in the individual newsgroups, or they can post their own messages. Many of the obscene or sexually explicit newsgroups are primarily categorized in the "alt." identified newsgroups. "Alt. is shorthand for 'alternative', indicating the fact that lifestyles and opinions can be extreme, and these are unmoderated groups with people writing most anything" (Laughon & Hanson, 1996, p. 16). The alt.sex newsgroups can feature explicit, erotic writing . Wallace and Mangan (1996) described this type of newsgroup as a place that has "no imposed boundaries - just a loose culture of sex-talk in which almost anything goes" (p. 65). Wallace and Mangan describe the evolution of this newsgroup:

The newsgroup had been created as a sort of rebellious joke in 1988. Due to a perception that there was too much volume on Usenet, and too little of value, an informal and self-appointed group of system administrators began in 1987 to take control, deciding which newsgroups would continue and which new ones might be added. One of their first acts was to reject a request for a drug-related newsgroup. An Internet pioneer, John

Gilmore, responded by creating the alt. hierarchy, in which anyone could create a newsgroup without the permission of the governing cabal. Alt.drugs was the first newsgroup in the hierarchy. The following year, Brian Reid added alt.sex and alt.rock-n-roll. (p. 65).

Another newsgroup category which often contains pornographic images is the alt.binaries category. Binaries is an indication that the files contain digitized pictures, photographs, and the potential for sound. There are many similar newsgroups on the Internet, and new ones are created daily. In many of the newsgroups, it is easy to determine the subject matter of the category according to the name (e.g., alt.bestiality). Other sites use names that disguise the objectionalities they may contain, so that a computer systems administrator would not be aware of its contents. Other communication resources may not be quite as accessible, but the fact that the material is not widely available can lead to more obscene information being stored there. More specifically, computer bulletin board systems (BBS) can contain pictures which can only be accessed if an individual knows the specific phone number to the BBS which has been previously set up by another computer-user. The danger of the BBS approach is that the obscene material cannot be tracked down by merely surfing the Internet, making it more difficult for police to locate the perpetrators. The fact that this information is not easily tracked is beneficial in the sense that the obscene information is not easily stumbled upon.

Incidences of cyberstalking on the Internet often emerge into cases of pedophilia. A pedophile may surf newsgroups in search of victims. Some curious young boys and

girls will correspond with individuals in such groups. The perpetrator may develop a cyber relationship with the child and seek to meet the child in person, in hopes of fulfilling his or her sexual intentions. If enough information is obtained by a stalker, an obsessive relationship may result. This can lead to cyberspace harassment. Computer pornography sellers may also go on-line offering to sell photographs of young children committing sexual acts.

As the number of users with access to the Internet increases, more people become exposed to these pornographic sites. A fear hovers that pornography rings will grow, become more organized, and perhaps be used to make big profits.

Copyright Infringements, and Fraud on the Internet

Copyright infringement is probably the most frequently committed criminal activity taking place on the Internet, despite the little attention it receives. Certain software, such as shareware, are put on the Internet for the sole purpose of being downloaded. Nevertheless, attention should be paid to what one is downloading, especially if the material is to be used for commercial purposes. In most cases, however, downloading a computer program or other materials from the Internet constitutes the making of a copy of a work and may potentially be a copyright infringement. In the United States, "the Clinton Administration has proposed that on-line transmissions of works, such as books and magazines, as well as computer software, should be expressly classified as 'copies' under the Copyright Law" (Kurz, 1996, p. 23). Undoubtedly, a website that downloads copyrighted material and then posts the material, or an individual who uses portions of copyrighted material from another website and posts it on his/her

own webpage, may be liable for an infringement of copyright laws. For the most part, people who commit this crime are not usually reprimanded. Copyright infringement is such a common practice that law officials cannot keep up with enforcement demands. Also, for the most part, self regulation is implemented for copyright circumstances. Nonetheless, Internet users should be aware of the rights held by individuals who copyright their material.

Scams in various forms are also harbored on the Internet. The Internet has created an emergence of stock scam artists. Prominently Canadian, many pyramid schemes are available on the Internet, with scam artists looking for naive buyers to cash in on the bull market. Typically, they are old scams operating in a new venue. The North American Association of Securities Administrators (Morton, 1996) reported a typical case in Alberta that occurred in 1994 where shares belonging to Wye Resources were being pumped through on-line chat rooms. Within a month, the share price was pushed from 20¢ to $1.40. The Alberta Stock Exchange then halted trading of Wye Resources (Morton, 1996). It is difficult for ordinary consumers to distinguish between the legitimate dealers and the bad. It is a challenge for officials to find the fraudulent perpetrators. If found, and a webpage is shut down, a new one may be set up almost immediately.

Another pyramid scheme was uncovered in Canada in the spring of 1996. In this scam, the Fortuna Alliance suggested that Internet users should become members of a co-op and share the profits. Gullible Internet users were asked to send $250 and then to sign up two new members. If instructions were followed, the users could expect money to

come their way in an amount exceeding $5000. However, no mention was made of the origin of the funds. The nature of this scheme is analogous to a chain letter. People are led to believe that if they send money, they will end up at the top of the pyramid, collecting from those at the bottom. Eventually, a federal court in the U.S. agreed with a request from the Federal Trade Commission of the U.S. for an injunction to freeze the assets of Fortuna. This was the largest case the FTC dealt with in regards to fraudulent marketing schemes on the Internet.

Hate Groups and Defamation on the Internet

The Internet has offered a new venue for hate and prejudice groups to express and to propagate their beliefs. The Internet has provided these groups with a powerful medium that reaches people from all walks of life. A deliberate search of websites reveals that these groups have a strong representation on the Internet. For example, white supremacist groups thrive in newsgroups and on websites, and many of these hate groups can be found thriving in the alt.revisionism newsgroup (Diamond & Bates, 1995). Bizarre religious groups have also made a presence within the confines of the Internet. Information on how to join various cults is readily accessible. The most recent case of this is the website devoted to the "Heavens Gate" cult of California, which advertised its beliefs on a self-made webpage. The demise of this cult evolved with a mass suicide of all thirty-nine members.

The Ernst Zundel homepage is perhaps one of the most well-known sites developed by a Canadian. This individual believes that the holocaust never happened, and most recently chose the Internet to convey these views. Because Zundel chose not to

protect his anonymity, he used an Internet access provider based in the United States. This allows Zundel to potentially avoid laws against hate mongering in Canada.

Wallace and Mangan (1996) quoted Rabbi Marvin Hier, who is part of an organization that tracks hate groups, regarding his belief of hate groups on the Internet. Heir stated that "Cyberspace offers direct, instantaneous, cheap mainstream, co nmur.ications in the marketplace of ideas. Further, young people - a target group for racists - are especially drawn to this cutting edge of technology" (p. 165). He further believes that on-line services should take measures to deny hate groups a forum in which to express their views. There is no doubt that these hate groups are most accessible to the young, who are the most likely age group to surf the Web. There is the potential for these hate groups to shape the minds of some naive onlookers.

Defamation is a topic which is at the top of the list in need of reform. This is due in part to its existence on the Internet, where it is commonly referred to as 'flaming'. Defaming people has become a sport of sorts on newsgroups, where messages are posted in regards to other users or individuals in public. There are debates in the courts whether this defamatory material on the Internet should be considered libel or slander. This issue will be discussed later in a review of Internet legalities.

Bomb-making Information on the Internet

The Internet has made the discovery of materials used to make bombs even easier than when printed materials were the most common resource. The Oklahoma City bombing and Unabomber cases in the United States have caused attention to be focused on bombing attempts. The speculation that the Unabomber utilized bomb-making

resources from the Internet has created an uproar over the degree of accessibility of this information. After the Oklahoma bombing, the media did not have to look far to find some bomb recipes. The introduction of the "Anarchists' Cookbook" on the Internet allows users to discover the ease of finding bomb-making materials - at your local hardware and grocery stores. Other on-line sources such as "The Terrorist's Handbook" provide detailed descriptions on how to construct lethal explosives, provoking people to experiment with the materials in their own homes.

Usenet features a newsgroup called alt.pyrotechnics, where users talk about the what it is like to set off explosives and give each other advice on constructing different types of bombs. Considering the ongoing court cases in the United States, the demand for similar newsgroups is likely to continue.

Hacking

A hacker can be described as a person with the intent to misuse or participate in mischievous activity on the Internet. Those with superb computer skills (hackers are usually intelligent teenage males) and a desire to cause some mischief have the potential to cause some havoc to various websites. Many hackers consider this activity as a game, and can do a lot of damage before they are tracked down. Recently, hackers humiliated the United States Department of Justice when they defaced the department's website, changing the title of the site from 'justice' to 'injustice'.

Security experts and hackers are similar in that they are both able to discover weaknesses in computer programs or systems. Dan Farmer, an American Internet security guru, created some controversy during an effort to promote awareness of existing

flaws in Internet systems. Farmer used a version of his own Internet security tool, SATAN, to conduct an unauthorized scan of 1700 websites held by banks, newspapers, federal agencies, and pornography sellers. Farmer reported that approximately two thirds of websites are "running bug-ridden software that make them easy targets for amateur hackers to disable and potentially damage" (Gibbs, 1997, p. 34). Farmer was not surprised that 68 percent of the websites held by banks, and 70 percent of those belonging to newspapers appear vulnerable to attack by hackers. There is need for concern on the part of all these types of establishments. As more people become computer literate, and more agencies maintain websites, there is a greater potential for an increase in hacking activities. Unless websites become more secure, there will be a bigger market for the expertise of people like Dan Farmer.

The Law

Canadian Law

Charging and prosecuting persons for offenses committed on the Internet is a most difficult challenge at present for a number of reasons. Unlike a typical crime scene, in an Internet crime there are no fingerprints, eyewitnesses, or blood trails. In addition, because few Canadian cases have gone to court, rules regarding evidence and legalities covering such crimes have yet to be firmly established. In consideration of the number of offenses likely committed, there is a need for the laws to be adapted to the crimes that have arisen due to this new technology. However, there is no consensus as to what is considered illegal. One of the government's last attempts to arrive at some solutions to deal with the crimes ended more than a year ago when the Canadian Information

Highway Advisory Council said the problems were "too numerous to recommend a course of action" (Coleman, 1996, p. A7).

Much of the legislation concerns pornography on the Internet, primarily due to the nature of the crime. When investigating pornography, not all should be considered obscene (Wolynski, 1995). The Criminal Code of Canada separates pornography into what is acceptable, and what is not acceptable. That which is not acceptable is labeled obscene. Specifically, Section 163(8) states: "For purposes of this Act, any publication is a dominant characteristic of which is the undue exploitation of sex, or of sex and any one or more of the following subjects, namely, crime, horror, cruelty and violence, shall be deemed to be obscene" (p. 2). Possession or distribution of child pornography is illegal. As George Sidor, an Edmonton City Protection Services detective maintains, " by making the overt act of saving it [child pornography] to your hard drive or diskette, you are now in possession" (personal communication, April 15, 1997). Obscene material showing sex and violence or bestiality is not illegal to possess, but it is illegal to distribute. It has been debated as to what constitutes distribution when computers are involved. It is questionable if downloading a file means possession, or if sending an e-mail constitutes distribution.

Although two men were charged in 1997 in Edmonton for distributing pornography, this is a rarity. Few such charges have been laid in Canada and there have only been two convictions at the time of this writing. These convictions came as a result of guilty pleas; there have been no trials. These statistics are about to change, as a trial began during the writing of this paper for the Edmonton case. Furthermore, during the

progression of the present study, another Edmonton man was charged with distribution of child pornography, and a young Albertan had a homemade bomb blow up in his face after attempting to set off a bomb he had learned how to build through instructions on the Internet. These low statistics may be partly due to the fact that police forces generally operate reactively in response to complaints. This approach generally coincides with law enforcement in Canada, as it is typically a reactive enforcement country. A proactive approach to dealing with these obscene communications would be expensive, time consuming, and would likely require more manpower than is available. Police officers, if in possession of a search warrant, can obtain e-mail and newsgroup postings, identify which websites have been visited, and determine a user's favorite web addresses. These actions can be taken following a complaint or a reactive investigation.

As police services are warned of the increasing dangers the Internet is bringing, some agencies are adjusting to its relatively new demand. In the summer of 1996, the annual report of the Criminal Intelligence Services of Canada warned about the potential of various crimes. The report noted that organized crime had begun using stolen telecommunication services to lead the way to other criminal activities, such as counterfeiting and drug-smuggling. Counterfeit credit cards have been found with membership numbers made from software programs. Losses due to these stolen telecommunications have been found to amount to more than $300 million a year. The report also notes that the laws involving telecommunication crimes are outdated, and "police forces are now struggling with how to walk a beat in cyberspace" ("Organized Criminals", 1996, p. A7). There is a concern that police departments may be afraid or

intimidated by Internet crimes, because of the technology involved. It can be difficult explaining technical information to judges or other law officials who are unfamiliar with computers or the Internet.

Due to the weaknesses in the Canadian legal system, it appears appropriate that Thomas O'Grady, current president of the Canadian Association of Chiefs of Police, believes "it is worth looking at the U.S.'s Communications Decency Act passed in February of 1996" (Coleman, 1996, p. A7).

Communications Decency Act (CDA) of the United States

In February 1996, the Clinton Administration signed the Communications Decency Act (CDA), a document that restricts the flow of information and free speech on the Internet. The CDA provides for fines of up to $100,000 and two years in jail for Americans who illegally distribute pornography on the Internet. This is a change from laws of previous decades which indicated that the printed word, including words on computer screens, could never be obscene. Only pictures and films were involved in prosecutions (Wallace & Mangan, 1996). Wallace and Mangan also noted that the CDA acknowledges the crime of making available "any obscene communication in any form including any comment, request, suggestion, proposal, or image regardless of whether the maker of such communication placed the call or initiated the communications" (p. 176). This section allows American prosecutors to charge individuals operating from other countries. Another provision involves the act of knowingly sending indecent communications to a minor. An Internet provider could not be held responsible unless

the provider knew about the activity, or authorized the activity. The issue of responsibility will be discussed in a different section of this paper.

The CDA is not without criticism. There are those who believe children will not be kept from indecency on the Internet, and that it will not be a flawless effort at regulating these indecencies. In June 1996, a court struck down the CDA, citing that it was unconstitutional. The CDA is still before the U.S. Supreme Court, as the decision is being appealed by the U.S. Department of Justice.

Cyberpatrols

There are some "Internet vigilantes" who are aiming to help legal professionals at tracking down illegal activities on the Internet. For example, the Cyber Angels are an offshoot of the Guardian Angels, a group based in Los Angeles. Many of the individuals belonging to this group have no previous experience with computers or communications. The organization boasts 1200 members worldwide, including 50 in Canada. Members of the Cyber Angels have been able to view first-hand the range of obscene material on the Internet, and the scope of illegal activities occurring in cyberspace. Members usually track the illegal activities, trace it, download it, and then turn it over to the police. Cyber Angels have discovered a problem when it comes to describing the problems to police forces. Many do not have a cyber-cop program. As Curtis Sliwa, founder of the group explains, "Most of them (cyber-cop programs) are in rural areas. Most of them are involved in sheriff's departments" in the case of the U.S. ("Angels on the Net", 1996, p. 36).

The Cyber Angels' hard work appears to be successful. They have turned over

information on over 5000 suspected illegal operations in á one year timespan. It is unknown, however, how many of the criminals involved have been charged.

When offensive material is distributed on the Internet, and its existence is made known to appropriate law officials, the debate arises concerning who is accountable for the activity.

Who Is Responsible?

The issue of accountability of the various crimes is a debate that will not be resolved anytime soon. Unless some specific legislation is devised, the issue will continue to flare, as the law is still murky on questions of accountability. The issue is one of determining if it is the responsibility of the system administrator (sysop), the individual, the company, or the school if, for example, criminal activities such as defamation or distribution of obscene material occur.

It is an unresolved debate in U.S. courts as to whether the owner or operator of an on-line system is responsible if defamatory statements are read by websurfers. As Kurz (1995) explained:

> Traditionally, 'distributors' (such as libraries, newsstands, or book stores), and common carriers (such as, telephone and telegraph operators) were not subject to defamation liability absent extraordinary circumstances. On the other hand, 'publishers' such as newspapers and publishing houses were responsible under the republication doctrine for the material they printed (p. 164).

To determine where the liability lies, it should be determined if an owner or operator of the service is a publisher, distributor, or common carrier. Distributors are not usually

held responsible for defamatory material unless it can be proven that the distributor knew, or should have known about the allegedly defamatory material.

If a service provider censors newsgroups, this illustrates knowledge of possible defamatory material, and the provider could be liable for any such material that was not removed. Conversely, if there was no effort at censoring, then the provider could be liable, due to the knowledge that there is likely to be defamatory material contained in the newsgroups. The provider must try to prove that he did not know, and had no reason to believe, that defamatory material existed in the newsgroups.

On the topic of liability of on-line services, a U.S. ground-breaking case was that of Cubby v. CompuServe (1996). The CompuServe on-line service features forums, or bulletin boards. Posted to one of the newsgroups was a newsletter called "Rumorville". Sometime later, Cubby Inc. began publishing an on-line newsletter called "Skuttlebut" which was competing with "Rumorville". Soon after, "Rumorville" accused "Skuttlebut" of stealing information. In response, Cubby sued CompuServe for libel. A Federal judge granted judgment to CompuServe, believing that CompuServe, as a distributor, was unaware of the libel. The judge concluded that CompuServe did not have any more control over the contents of its messages than any other distributor, and it would not be feasible for CompuServe to view the contents of each file.

The first known case of an arrest being made against a sysop for illegal material on a BBS involved an individual in California. A stolen credit card was posted on the sysop's BBS while he was away. The sysop claimed he did not know about it, and did not encourage such actions. The charges were eventually dismissed when members of

the public vehemently educated the police that the sysop's policy on disapproving of illegal materials on his BBS should have been enough from protecting him from liability (Wallace & Mangan, 1996).

In Canada, charges of distributing obscene material can be undertaken against the system administrator of a bulletin board system if it can be established that he/she possessed knowledge of the contents of the distribution. This can be difficult since it is unreasonable for a sysop to examine the contents of all BBSs, and the names of some files may mask their true contents.

However, this scenario becomes difficult when network services outside Canada are involved. Because the Internet has no boundaries, jurisdictions are easily and rapidly crossed. This adds greater uncertainty as to who should be responsible for illegal activity, and makes the idea of regulating the Internet seem impossible.

Arguments For and Against Regulating the Internet

The need and feasibility of regulating the Internet is another debate that rages as the Internet becomes more popular and accessible. Just as strong, is the argument that censorship infringes on peoples' rights. Dual sides of the argument were described by Johnson (1994):

> We can imagine a Cyberspace in which everything you 'say' or do is monitored by law enforcement officials, so that you must anticipate that anything you say on-line may someday come back and haunt you. Or we can imagine a Cyberspace that realizes the dream of democracy, in which individuals freely exchange information of importance to them, without fear of repercussion

> so that they are able to learn from one another and openly debate the issues of the day (p. 42).

The issue concerns freedom of expression on-line and how much power the government or law enforcement officials should have to control on-line activities. Some fear that an absence of privacy would diminish the Internet's democratic spirit. Others take it a step further, and believe that regulating the Internet is a form of Fascism.

In a Southam-Global poll of adult Canadians conducted in 1997 (Cobb, 1997), 66% of the adults responded that they favored the government passing laws to regulate Internet access.

For those against censorship, section 2(b) of the Canadian Charter guarantees "freedom of thought, belief, opinion, and expression, including freedom of the press and other media of communications" (Wolynski, 1995 , p. 2). However, these rights are subject to reasonable limits, so the government can restrict the freedoms in certain circumstances.

Whether it be the government, individual users, or groups like CyberAngels, the Internet does provide evidence that some type of regulation or policing is required when the scope of criminal activities being committed is considered. There is little or no control over the content of material posted over the Internet, at least not by the Internet itself. Therefore, it is up to those with access to the Internet to use "netiquette". Rules or laws enforced by authority can only do so much; what is needed most are responsible users. Although many Usenet providers carry obscene newsgroups and have the capability to restrict certain newsgroups, the Internet shuns censorship, and in most cases,

prefers to police itself. Therefore, users are expected to demonstrate a degree of netiquette. Users should report suspicious-looking behavior to others - system operators, or other users. Johnson (1994) believes this responsibility should be extended: "Users of a system should periodically discuss what is happening on-line and how to make the system work better" (p. 50).

There is evidence that some Internet providers have chosen to take a proactive approach to the removal of obscene material they make available on-line. For example, Internet Connect Inc. of Edmonton, Alberta pulled over a dozen newsgroups from its server because of concerns related to liability. The systems manager did not see the act as an infringement on free speech "because the information is still available on the Internet through other service providers" (Gold, 1996, p. H2). Another Edmonton Internet provider, OA Internet Inc, decided not to block any access until asked to do so by the police. Other companies such as CadVision and the Internet Centre from Edmonton operate two servers - one censored, and one uncensored. This approach is an effort to allow users to decide on their own what they want to see (McCarten, 1996). Removing newsgroups, however, may not be the best solution. Users can post information on other groups with less obscene titles. This can provide for little control of the content on the newsgroups, and a constant monitoring of all groups is unreasonable. In addition, the Internet has no jurisdictions; it is international, and the material cannot be stopped at the border. Information on the Internet may have been placed there by any person from any country, and is available freely to another user anywhere in the world. What is illegal in one country may be legal in another. "German law prohibits claims that the Holocaust

did not happen, but this does not prevent white supremacists in the USA or the UK from transmitting this claim to their sympathizers in Germany" (Burton, 1995, p. 416). If any type of control is to be implemented, international cooperation would be a necessity

Although there is a group of Internet users who would like to make it friendlier for themselves and other users, there is also a group which believes a secure system would disrupt the free flow of information - an intrusion they are not ready to accept.

Background to Study

A group of students from a college in Minnesota (Rasmussen et al., 1995) conducted a case study examining pornography on the Internet, and the policies of various colleges in Minnesota. The directors of academic computing facilities for both public and private institutions were surveyed on their positions of regulation, so that the authors could determine what preventive measures were taken by these officials concerning pornography on the Internet.

Rasmussen et al. used Gustavas College as their control group, where they also interviewed the Dean of Students and UNIX system operator. These officials could potentially verify the responses of the system administrator, thereby having a unified opinion concerning policies. The system administrator of each institution was asked about the policies the college currently followed, and if any future changes were expected to be made to that policy.

The University of Minnesota, a public institution, implemented a policy in which a disclaimer message appears before any link to their system. This disclaimer, which was suggested by the FBI, states that the University of Minnesota has the right to look at

anything on their system, and will report all illegal activity. The university voiced the belief that the policy has been successful to date. The university's position on pornography follows that of U.S. federal laws, but they do not limit system use. The director of computing services at the university expressed the belief that there may be limits implemented in the future (Rasmussen et al., 1995).

Mankato State University, also a public institution, did not have a current Internet use policy. The director of computing services felt that because Mankato is a public school, it would be in violation of the First Amendment if they controlled students' access to look at pornography on the Internet. He further believed that it was not the university's position to make that moral decision for its students. However, if problems arose due to pornography on the Internet at his university, the director would turn the problem over to police.

At Gustavus Adolphus College, a private institution, there was no monitoring of Internet activity by the director of the Academic Computing office. The policy Gustavas used provided for no censorship. The UNIX systems administrator also supported the view of not limiting students' Internet use, stating that it would be technically impossible to limit use, and pornographic sites. The administrator cited that he believed most of the pornography took place on newsgroups, which were changing daily, and on private bulletin boards. The Dean of Students at Gustavas believed that students must take on the responsibility to police themselves, according to specific guidelines. He believed these guidelines should be stated in a disclaimer at the beginning of each homepage stating that the text expressed does not reflect the institution (Rasmussen et al., 1995)

St. Olaf, a private institution, only used one type of blocking. There was no blocking service of any newsgroups, but blocking was implemented for creation of homepages. Any variety of pornography or obscenity was not allowed. However, enforcement was based solely on the 'honor system'. The Academic Computing office ensured privacy of a student's files, unless policies had been violated. Then, a note granting permission to access files was provided by higher officials. Furthermore, when a student received an account, they were asked to sign a 'Statement of Responsibilities' concerning misuse of computers, unauthorized copying of software, international network etiquette, and account privacy before accessing use (Rasmussen et al., 1995).

At another private institution, Bethel, students were required to sign a waiver indicating they understand the lifestyle expectations at Bethel College, including ethics of computing. There was no monitoring of computer usage, and inappropriate use was handled through the honor system. However, a policy of what it means to be a "good citizen" had been implemented at the college to deal with Internet matters. The policy provided a listing of what was considered good behavior on the Internet. Concerning the issue of homepages, the college added a disclaimer at the beginning of all homepages explaining that it is the creation of the student, and does not necessarily reflect the views of the college. The system administrator at Bethel believed that the policies enforced by the college had been successful.

Overall, Rasmussen et al. concluded that the colleges did not view pornography on the Internet as being a problem. The public institutions need to abide by external social laws, and the private institutions have the option to follow any moral standard they

decide upon. The reputation of the institution seemed to be an underlying theme in all policies implemented.

Although the study by Rasmussen et al. (1995) offered an informing examination of the measures some institutions employ to regulate the Internet, much more could be learned with a larger sample. Also, the questions asked were not very comprehensive, and some additions here also may have been helpful. Although pornography is perhaps the biggest problem on the Internet in regards to severity of crime and deserves to be a focus of Internet crime research, much insight would have been gained from an analysis of a variety of criminal activities on the Internet.

Another research project that focused on Internet pornography was conducted at Carnegie Mellon University (Rimm, 1995) and revealed some startling findings. During the course of the 18-month study a total of 917,410 sexually explicit pictures, descriptions, short stories, and film clips were discovered. Using computer records of on-line activity, the author was able to measure what people actually downloaded. Rimm concluded that 6.4 million pornographic items have been downloaded or called up by computer users, and that over 70 percent of the sexual images on the newsgroups originated from bulletin board systems that were adult-oriented. When Rimm examined global Usenet usage, he reported that three of the five most popular newsgroups were pornographic, and that 20 percent of the posts in the top forty newsgroups were pornographic.

The Carnegie Mellon study also identified individual consumers of the pornographic material in more than 2000 cities in all 50 American states and 40

countries, Canadian territories and provinces; 98.9 percent of the consumers of on-line porn were men. While these statistics may appear overwhelming, the study carefully points out that despite the popularity of pornographic image files, they constitute only about 3 percent of all the messages on the Usenet newsgroups, while the Usenet itself represents only 11.5 percent of the traffic on the Internet (Rimm, 1995). These statistics were overshadowed when an article in Time magazine addressed the findings of the study conducted at Carnegie Mellon. The article (Elmer-Dewitt, 1995a) cited what would become a very controversial statistic from the Carnegie Mellon study when he reported that "On those Usenet newsgroups where digitized images are stored, 83.5 percent of the pictures were pornographic" (p. 1850). However, critics have pointed out that Rimm only counted the images of selected newsgroups, but caused misinterpretations of his findings when he reported in his summary that 83.5 percent of pictures on newsgroups was pornographic which was an overgeneralization.

The study resulted in the administration of Carnegie Mellon University banning many newsgroups that were sexually explicit. The president of Carnegie Mellon feared that the university could be prosecuted under state pornography laws if access was not controlled. This censorship started an outcry from students who were outraged by the decision, citing their First Amendment rights. The university decided to restore the text-only newsgroups, but not those carrying photographic images.

The research by Rimm (1995) and the Time magazine article (Elmer-Dewitt, 1995a) addressing the findings of Rimm, have brought a wave of criticism and controversy.

Rimm did not make a clear distinction among the Internet, bulletin board systems, and newsgroups. Rimm sometimes "lumps" statistics together as a whole from these sources, although they cannot be so easily compared. In an on-line critique of the articles by Rimm and Elmer-Dewitt (1995a), Hoffman and Novak (1995) contended that the Time article by Elmer-Dewitt, contributed to this confusion, and gave the Rimm article more credibility than it deserved. Elmer-Dewitt wrote in the Time article that "there is an awful lot of porn on-line" (p. 33). Most of the data presented by Rimm was obtained from adult BBSs, which was a very minor portion of "on-line" material, and did not include the Internet. Other critics have reported that Rimm exaggerated the availability of pornography on the Internet by combining findings from private adult BBSs that were restricted to minors and required credit cards, with those from public networks, which were not restricted to minors (Elmer-Dewitt, 1995b).

The methodology used by Rimm should also be viewed with some skepticism. For example, the tracking behavior to determine which sites computer users viewed, was measured over only one time period – January (1995). Because behaviors could change during different months, a time-series approach would have been more appropriate. As Reid (1995) stated in an on-line critique, "student interests in January are extremely different from student interests in September or April." In addition, the results of the study by Rimm would be difficult to replicate. The methodology is presented with little detail, and it is sometimes difficult to determine how the results were obtained. Finally, although the title of the Rimm article is "Marketing Pornography on the Information

Superhighway", the issue of marketing is given minimal discussion. Any viewpoints that are presented on marketing, are not supported by any literature.

Although the article by Rimm (1995) first appeared to be a groundbreaking study that justifiably created panic in those individuals who know little about the Internet, and those who did not scrutinize the article, the criticisms have greatly downplayed any valuable insights the article may offer. It is true that the public should be concerned about the existence of pornography in cyberspace, but the study by Rimm exaggerated this claim, and provokes questions regarding the research methods employed.

A study conducted in Scotland offers a most informing view related to regulating the Internet. Burton (1995) examined both the need and feasibility of regulating the Internet through a two-part survey into the topic. The overall aim of the Burton study was to assess the extent to which self-regulation was exercised, and to determine if there was evidence that Internet providers were controlling access to offensive materials. In addition, Burton wanted to determine if sites were having restrictions placed upon them by some authority, and on what basis. To investigate these questions, offensive topics such as abortion, drugs, war, and pornography were chosen (p. 418).

Associated newsgroups related to the offensive topics were scanned and webpages were found by use of search engines. Burton (1995) found that essentially no control of newsgroups and webpages existed for the topics of abortion, drugs, and war. When contributions to lists were checked, it was only to ensure that they were relevant to the topic, not to censor them. Burton found evidence that if someone did not follow ethical conduct, they may be subject to public criticism on newsgroups or websites, or the

collapse of their e-mail system could occur due to being deluged with huge files. Only in the case of pornography/erotica was there any indication of some sort of regulation.

Burton (1995) found sixty-five sites overall on the World Wide Web which contained images that could cause offense. "The type of material found in the survey of websites was wide-ranging, and there was a concomitant variation in ease of access" (p. 419). Burton found that some sites and links to sites contained warnings of nudity, or that the files should only be viewed by people over eighteen or twenty-one, and that they may be considered illegal in some countries. In most cases, however, there was no prevention taken to ensure that these warnings were not ignored. In any case, these warnings could be said to lend some support to the idea that the Internet is imposing some measure of self-regulation. It could also be said that the warnings could feed curiosity and lead to access. On one commercial site when users were asked to give their age, it made no difference if an individual was a minor. The user was still connected to sites containing adult material.

Nineteen of the 65 sites placed no limitations on access to non-explicit material. These sites included photographs of models which ranged from fashion photographs to full nudity. On these pages, there was an indication about the nature of the material stored there.

Seven sites from the total of 65 appeared to contain explicit material. Of the four which exercised some control, two were pages maintained by individuals attending European universities. In both instances, a password had to be obtained from the owner

of the page. Another site that controlled access was a commercial provider, which gave no evidence that checks were made to ensure that no minors obtained a password.

Three examples of sites having no regulation of access and containing explicit material were located. Two of these sites contained a warning at the main directory of the file, but it was possible to bypass this warning and access the files. The third site was an on-line art magazine featuring explicit photographs and text. In twelve cases, access to a link provoked a "403 Access forbidden" message, suggesting that permission must be granted from the site owner before accessing the site. Also, problems coping with high demand was the most frequent reason given by the thirteen sites that were shut down. Of other sites that were shut down, the reason was due to a closure of the site by university administration.

All of these sites were tracked down with relative ease. Burton (1995) discovered that explicit sites formed a small percentage of the total, and most of these had some form of regulation in place (although not always effective). Burton concluded that the most accessible files contained images which could more easily be found in bookstores. Sites that featured explicit images tended to be protected by passwords. In addition, Burton felt that if all sites were managed responsibly, " there would be some justification for the view that imposed legislation is not necessary" (p. 422). Burton found that the university sector exercised the greatest amount of control.

The second part of the Burton (1995) study consisted of a short questionnaire sent via e-mail to various British universities, as the university sector in the UK represents the largest Internet group. Questionnaires were sent to all British universities operating

World Wide Web pages, and for which an e-mail address could be found. The results were based on 34 useable responses (50 percent response rate).

The survey presented to universities consisted of multiple choice questions such as: How is access restricted, if applicable?, Reason for controlling access, Is this policy made known to users?, Is the policy strictly adhered to, and under what circumstances can the policy be relaxed?, How was this policy devised, and did any consultations take place with the concerned parties?

Burton (1995) found that 62 percent of the respondents exercised no control over access to the Internet. Twelve of the 34 universities exercised some type of control, with one university controlling access by students. Eight (24%) of the universities that had a policy on access, made their policy known to users, and eight did not. Of the seven (21%) universities which would relax the policy, three universities would do so if the reason was for staff research, and one if it were for student research. Reasons given which were not options on the questionnaire included if there was more disk space, or more bandwidth, "indicating that content of files was not the main criterion on which limits were based" (p. 423). A third reason indicated that a policy would be relaxed if person in authority gave the order. Ten universities (30%) had arrived at the policy of access as a result of a decision by Computer Services, and eight more as a result of a decision made by central administration or some other university committee.

When asked for additional comments, seven respondents suggested that regulating access to the Internet would be difficult, due to technical problems, and the amount of time an endeavor like this would take. In general, the comments made by respondents

fell into two groups: "recognition of the difficulties inherent in controlling access to the Internet, and permitting open access subject only to the general university regulations on computer use" (p. 425).

Burton (1995) noted that there were certain methods on how to approach regulating the Internet that would be most appropriate. He wrote, "if we simply approach the problem as one of suppressing material, we will lose more than we gain" (p. 425). He believed that if we clarified that the contents of a webpage are offensive, then users would be left with a choice of whether or not they wanted to view the material. "For most Internet users, there is always the choice not to read material which is clearly identified, just as there is always the choice to switch off our television sets or not to buy printed publications" (p. 425). Burton argued that regulation of the Internet has the potential to harm the free flow of information that the Internet can provide on such a global scale. The Internet is much too valuable of a resource to damage in some way.

The Burton (1995) study provided some enlightening viewpoints into the feasibility of regulating the Internet, and the need for some control. The survey of various universities to investigate policies into regulation resulted in some valuable insight into what measures are currently taken to enforce these policies at UK universities, and the debate surrounding the issue of controlling access, or not restricting access. A similar study conducted with Canadian universities could prove useful in ascertaining the policies implemented and the positions taken in regards to regulating the resources of the 'information superhighway'. The method used by Burton to obtain the surveys was somewhat problematic, however. Burton wrote that questionnaires were sent

to those universities which were operating webpages, for which an e-mail address could be obtained. It is unclear as to which university official completed the survey, and if this choice of respondent was uniform across all questionnaires completed.

Summary of 'Gaps' in Literature

To date, there has been little Canadian research on the topic of crimes on the Internet, and the subject of regulation of the Internet. Although studies from Europe and the U.S. have offered many insights, Canadian research is warranted. Governments in both the U.S. and Canada are still grappling with laws which have not been firmly established regarding the Internet, and the regulation debate rages on. It is the intention of this author to provide some viewpoints into the issue of Internet regulation, and to see if any type of resolution is possible. For example, the safety of the Internet is an important concern to teachers and parents due to the effect its impurities could have on young people. There is a paucity of research warning of the problems and measures role models can take to prevent access to obscene materials. More research could serve a useful function in making potential criminals aware that studies are being done to prevent abuse of the Internet, and to warn others of the existence of such abuses. This is the intention of the author of the present study.

Purpose of Study

In an effort to gain insight into the issue of regulation of the Internet, the author examined the existing policies of various Canadian universities, and the preventive measures that academic computing system operators take concerning obscenities on the

Internet. The issue of Internet regulation and policies will also be examined for Alberta school districts.

The author will also examine the prevalence of Internet crime investigations by various police services in Canada and the viewpoints of the police on the issue of Internet regulation.

A final purpose of the present study is to increase the potential of raising awareness of methods parents and teachers can use to prevent access to obscene material on the Internet by young people.

Chapter II

Method

Subjects

School Officials - The sixty-five school districts in Alberta were targeted as participants in the study. Of these sixty-five, fifty-two Superintendents, or other head officials, returned completed surveys (80% response rate). All participants were volunteers, and identities remained anonymous.

University Officials - Directors of Computing Services at 15 universities in Canada were recruited as participants. Twelve surveys were completed and returned (80% response rate). All participants were volunteers, and their identities remained anonymous.

Police Departments - Fourteen police departments across Canada were recruited for the study. Eleven surveys were completed and returned (79% response rate). All participants were volunteer, and identifies were kept anonymous.

Survey Instruments

School questionnaire - A short survey consisting of 10 questions approximately 15 minutes in length was sent to appropriate school officials. Both open and closed questions were included in the questionnaire. The content of the questionnaire was a modified version of one developed by Burton (1995). It probed school officials' implementation of restricted access to Internet sites and their comments on regulation. (See Appendix A).

University questionnaire - The short survey sent to university officials was

identical to the school questionnaire except for minor modifications to the survey to make it applicable to a university setting. The survey consisted of 10 questions and was also approximately 15 minutes in length. (See Appendix B).

Police questionnaire - This survey also consisted of 10 questions which could be completed in approximately 15 minutes. It included both open and closed questions, and explored each police agency's views on regulating the Internet and the prevalence of various Internet crimes. (See Appendix C).

Procedure

Universities targeted for completion of the university questionnaire were chosen based on the student population of the institution. The largest university from each of the 10 provinces was selected. In addition to these 10, the next 5 largest universities in Canada were chosen. (See Appendix D for a list of universities included in the study). Letters of explanation, the questionnaire, and a self-addressed stamped envelope were sent to Directors of Computing Services, or similar officials, at each of the universities. Addresses, titles, and name of officials, when available, were obtained on the Internet.

It was documented in the letter of explanation accompanying the questionnaire that completion and return of the questionnaire signified consent to participate in the study. Ethical clearance and assurance of anonymity were also included in the letter. Similar letters were sent with the school and police surveys as well. (See sample of letter of explanation in Appendix E).

Approximately three weeks following the initial mailing of the questionnaires, the questionnaires were resent to all universities included in the study. The questionnaires

sent for the follow-up were identical to those sent in the initial mailing, but revised letters of explanation were included. The same revised letter was also used for the follow-up of the police and school questionnaires as well. See Appendix F for this letter. The initial response rate was 53%. This increased to 80% after the follow-up.

Targeted police departments were selected by first recruiting those agencies which were believed to have a unit devoted to investigating Internet crimes. These police departments were determined via information provided by Det. George Sidor from Edmonton Police Services, and from information obtained on the Internet. The remaining agencies were selected based on a stratified sample of the 10 provinces. The size of the centre where the agency was located and the possibility of a departmental focus on Internet crimes, as conveyed by Internet information, were the deciding factors in the selection. Contact names were used when mailing the questionnaires, when such information was available. See Appendix G for a listing of agencies which were targeted. The mailing process used for the police questionnaires was similar to that used for the university sample. The initial response rate was 50%. This increased to 79% with the follow-up questionnaire.

The school questionnaires were sent to school districts in Alberta. Contact information, including addresses, was obtained from a current listing made available for a small fee from Alberta Education. See Appendix H for a listing of school districts included in the study. The same mailing procedure was used for this questionnaire, as with the university and police samples, except that a stamped, addressed postcard was included with the questionnaire. Participants were asked to return the postcard which

contained the school name on the card, separately from the questionnaire. This allowed the researcher to determine if a questionnaire from a particular participant was returned, while still preserving the anonymity of the participants. This process facilitated the follow-up or second mailing, as the researcher knew to whom not to send a subsequent questionnaire. Approximately three weeks following the initial mailing of the questionnaires, the researcher determined who had not yet returned their questionnaire by checking the postcards, and follow-up questionnaires were sent, as well as a stamped, addressed return envelope and postcard. The initial response rate was 62%, which increased to 80% with the follow-up. Two questionnaires were returned by the postmaster due to a change in mailing address. These addresses were subsequently updated and the questionnaires were resent.

Chapter III

Results

Police Questionnaire

Frequencies and percentages were computed for the various responses on the police survey by using the spreadsheet program Excel 7.0 for Windows. Furthermore, various comments were made on the returned surveys, as well as qualitative responses to open-ended questions. Similar themes were evident among the comments made by the various participants.

It was determined that fraud on the Internet was viewed as the most prevalent Internet crime. Eighty- three percent of the surveyed police departments rated fraud as being the most prevalent crime. Besides crimes such as fraud, child pornography, distribution of pornography, defamation, and copyright infringements, participants also noted threat/hate propaganda, mischief, destruction of data, hacking, and pyramid/telemarketing as other crimes currently being investigated. All police respondents (100%) rated fraud as being the most often investigated crime. A comment was made that although fraud is investigated most often, "pornography gets the most publicity." Other Internet crimes listed by the participants as being most often investigated included mischief - unauthorized use of Internet service, theft of telecommunications, and hacking.

The number of charges laid due to Internet crimes in the 12 months prior to the completion of the survey ranged from the category 0-4 to that of 15+ (Please see Table 1). Six out of 10 of the respondents reported that there have not been any convictions

related to these charges. The number of complaints currently being investigated ranged from 0-4 to 15+ (Please see Table 2).

Table 1

Number and Percentages of Charges Laid in Past Twelve Months due to Internet Crimes as Reported by Police

Charges	Number	Percentage
0-4	8	73%
5-9	0	0%
10-14	0	0%
15+	3	27%

Table 2

Number and Percentages of Complaints Currently Being Investigated as Reported by Police

Complaints	Number	Percentage
0-4	6	55%
5-9	3	27%
10-14	1	9%
15+	1	9%

Of the 11 respondents, five reported that they have never taken a proactive approach to fighting Internet crime. Regarding reactive enforcement, one participant commented "this has only been very basic though, due to finances and person-power. We have made contact with all local ISPs and developed them as sources of information/contacts and encouraged them to contact us with any problems they experience." On a question concerning the feasibility of regulating the Internet, 6 out of 10 of the respondents reported that they do not believe regulation is feasible. Many of the comments regarding regulation concerned the issue of global agreement in the investigation of Internet crime. One participant responded "with a global understanding of the Internet and implementations of international agreements dealing with jurisdictions and enforcement, this is possibly leading to an international body to coordinate investigations when they exceed the boundaries of the involved countries." The need for a similar type of enforcement conveyed by another participant was that a : "Regulating body to govern Internet content [is needed]. Strict penalties. Government agency (Federal) to investigate and prosecute violations." Similar sentiments were expressed by other participants such as

- "Regulating the Internet will not be achieved unless [there is] worldwide political commitment and agreement."

"International treaties/laws must be addressed by government. Firewalling all countries who don't participate."

The scope of the issue is suggested by the following comment: "This is a

worldwide issue -unless political difference could be resolved.....[It is] too large, too many jurisdictions, current state not feasible."

The issue of jurisdiction was also alluded to in comments made about regulation. For example:

- "the Internet can be regulated but only to a certain degree. The biggest problem stems from jurisdictional issues. Laws enacted in one country might not be paralleled or adhered to by another because of differences in laws and culture of another country."
- "very hard since the Internet knows no geographical boundaries. The actual technical nature (TCP Protocols) makes it impossible to regulate."

Feasibility of regulation was questioned in another comment: "How can a small individual force police something like the Internet when it can cross provincial, federal, international jurisdictions? I don't think police or prosecution lawyers have enough knowledge regarding Internet crimes."

Suggestions on the set-up of the Internet were made by some participants. For example:

- "[Need to] start over and encrypt everything. Regulate all servers to (1) give law enforcement access to all their records (2) make applicants prove identity, etc."
- "There needs to be two distinct Internets: (1) The current Internet (nonsecure) and (2) a non TCP Packet and be secure for commercial transactions."

A hypothesis was also given as to how the Internet will be set up in the future: "The Internet will, one day, be regulated like the satellite TV is today. But until that time, it is a free for all." Solutions such as "parental control" were suggested as well as ideas for

dealing with the problem: "We will have to lose our current paradigm of how we deal with offenders, witnesses, etc. We will have to find new innovative ways of handling this type of crime."

When asked for comments on the issue of Internet crime, many comments on the magnitude of the problem were given. These included:

- "It is growing faster than any other crime. Education is the best method for getting this information out,"
- "It has only just begun!,"
- "It's going to get worse!,"
- "On the rise, will be the crime of the future."

The challenge facing police departments is expressed in comments such as:

- "Smaller police agencies do not have manpower, training, resources, to do proactive policing or reactive, for that matter,"
- "Right now the quality of information on the Internet can be questionable as to what is editorial, advertising, or outright fraud. No government is staffed or equipped to regulate the Net on its own under its current state. Thus, much of the regulation must be done by the public users. The problem with this is to regulate things consistently so that some do not take a vigilante approach."

University Questionnaire

Frequencies and percentages were computed for various responses on the University questionnaire. Responses indicated that most often there are some restrictions placed on all users' access to the Internet at Canadian universities (See Table 3). The

most common reason cited for controlling this access to sites on the Internet or newsgroups was concern over the size of files (6 out of 7 responses). Many institutions which restricted access, controlled access to the alt. newsgroups, both due to the nature of the files and the size of the files. Similar procedures for restricting access were followed by the respondents (See Table 4). One participant reported that the policy could be relaxed if requested since "If anyone needs access to any such newsgroup, they could request it and we would likely comply. During the Homolka trial, we denied access to the alt.fab.karla.homolka newsgroup due to the outstanding court ordered ban on publication." Others may restrict binary newsgroups but "We don't carry binary groups on our server due to lack of resources. We control access to IRC during peak hours to reduce contention for the modem pool, but we allow this from midnight to 8:00am." Responses further indicated that this policy on restricting access was most often developed by central administration (50% - 5 out of 10) or by another body or group such as Steering Committees, or Senate Committee (50% - 5 out of 10). Most often there was no consultation (5 out of 9). Overwhelmingly, most respondents believed that their policy was successful. Of the 10 respondents, 90% indicated a success rate.

Table 3

Number and Percentages of Universities Reporting Restrictions on Internet Access

Restriction	Number	Percentage
No control exercised	2	17%
Some access by students controlled	0	0%
Some access by staff controlled	0	0%
Some access by all users controlled	10	83%

Table 4

Number and Percentages of Universities Reporting Various Procedures for Restriction of Internet Access

	Number	Percentage
Filtering program used	No 9	100%
	Yes 0	0%
Policy made known	No 1	10%
	Yes 9	90%
Can relax policy	No 2	20%
	Yes 8	80%
Policy relaxed for staff research	No 3	30%
	Yes 7	70%
Policy relaxed for student research	No 3	30%
	Yes 7	70%
Policy relaxed for other reason	No 7	70%
	Yes 3	30%

The consequences for breach of policy were varied according to comments given. According to one participant, breaches are "handled under University Discipline Code for Students and various Labour agreements. For students, typically this involves a meeting with the Dean of Student Affairs and Services. A reprimand and a letter of apology is often requested." According to another participant, consequences include: "For students, suspension or expulsion. For faculty and staff, loss of pay, possible termination." At other institutions, no consequences apply "Not applicable - this policy is implemented via technical means" and "the policy is that these newsgroups are not distributed by the university's NewsServer. No consequences apply."

School Questionnaire

The frequencies and percentages were computed for various responses on the school questionnaire. Responses indicated that there are some restrictions placed on access to the Internet in school districts for all users (See Table 5). The most common reason cited for controlling access to sites on the Internet or newsgroups was concern about the moral, ethical, religious, or other nature of the files (26 out of 30). Many of the participating schools responded that they rely on professional judgment of parents, teachers, and responsible conduct of students for regulating use. Some participants noted:

- "Filtering is determined first by their weekly updated file. We then modify the control list to ask input from teachers - we open or close any site requested by a teacher as it is their professional judgment."
- "[We] control sites such as porno, sex, or related sites due to parents' concerns, chat sites due to bandwidth issues."

- "Policy on computer network Acceptable Use provides direction to students, staff, and community measures regarding unacceptable material."

The degree of restriction to access varies among districts, as conveyed by the comments:

- "...varies from school to school. Best control for secondary schools considered to be log of sites visited by individuals - regularly reviewed."
- "[the policy] is the responsibility of each school."

Table 5

Number and Percentages of Schools Reporting Restrictions on Internet Access

Restriction	Number	Percentage
No control of access exercised	8	15%
Some access by all students controlled	11	21%
Some access by staff controlled	0	0%
Some access by all users controlled	33	63%

More intense restrictions are placed in some of the schools as expressed by the comment: "we do not allow students to have Internet accounts. Students can only use the Internet under direct teacher supervision." The moral content of sites and the decision to regulate some of these sites was commented on a number of times. As one participant noted "We wish to prevent access to websites with sexual content (e.g., Pamela Anderson sites, porn sites, Neo-Nazi bomb-making sites). We currently do this on some K-9 computers. We do not want the students to access this material because of the moral and ethical content." Religion also contributed to these beliefs about morals: "We are a Catholic School District and as such believe we must live/work and uphold the teachings of Christ as an example to our students." A number of respondents commented on the fact that they restrict the Internet by means of chatrooms and newsgroups. For example, one participant commented, "Kids: All newsgroups due to cross-posting problems, all chatgroups, all sites blocked by screening software. Staff: Non-educational use is prohibited."

Other school districts suggest that they do not exercise any restrictions:

- "Spelled out in policy - not particular sites as they constantly change."

"No specific sites [controlled], by general rule of good taste, acceptability, etc." Quite similar procedures of restricting access were followed by most of the respondents (See Table 6). It was suggested by many of the comments that if a software screening program was not presently in use, there is some method of limiting access in the process of being implemented. The program Surfwatch was named by most of the participants who chose to respond to the question pertaining to the purchase of a program for limiting

access. Programs such as WebSense and CyberPatrol were also mentioned. In some cases, "The software varies among schools and, therefore, site access varies as well." Economics was suggested as a factor in the decision to implement a software program: "We use a vendor supplied filter list - WebSense, as we have decided this is the only cost-effective means to implement at our Internet ." Responses further indicated that this policy of restricting access was most often developed due to a decision by a body or group other than central administration or computer consultants (59% - 23 out of 39). Some of these groups included technology coordinators in schools, teachers and parents, or Board of Trustees. Most often, the groups affected by the policy were consulted. Eighty-one percent of the respondents indicated they consulted (34 out of 42) with the affected groups. A number of comments suggested that both parents and users are involved in the signing of agreements: "..all users sign a User Agreement" and "Acceptable use developed on school by school basis and students informed and sign agreement with parents." The consequences of the breach of the policy ranged from a verbal reprimand to zero tolerance resulting in expulsion. The most common consequence was a loss of Internet privileges, as expressed in the following comment: "We have an Appropriate Use agreement which details what is appropriate/inappropriate and consequences of breaches of agreement - suspension, expulsion, loss of computer privileges." Another participant stated, "Usual range of discipline, including withdrawal of access, possible suspension to expulsion/termination (staff)." Loss of privileges was also cited by another district representative: "Disciplinary action is determined at the school, depending on the offense Suspension of students and loss of access period.

Discipline action leading to possible dismissal of staff." These consequences have been implemented within one participating district: "Access would be denied. One of our subcontractors has terminated an employee for illegal use of our (School Board's) Internet services." Of the 32 participants who responded to the question relating to success of the policy, 100% indicated success. Most of those who did not respond commented that because their policy was very recently developed, it is too early to tell if it will result in success. When asked to comment further on the issue of regulation of the Internet, varying views on responsibility were expressed. Some conveyed that it is the responsibility of the user, others suggested it was the school staff. Comments supporting user responsibility include: "Self-regulation and training people to be knowledgeable about the Internet are crucial..... We are early in the implementation process and would anticipate putting some restrictions in place as time and resources become available. Need to track sites, responsibility on users." Comments supporting staff responsibility include: "Control by monitoring by staff and Internet access form which is signed by students and parents." In addition, "Educating kids about potential dangers, which accessing Internet resources and how to deal with these situations, is the only long-term solution."

Table 6

Number and Percentages of Schools Reporting Various Procedures for Restriction of Internet Access

		Number	Percentage
Filtering program used	No	13	32%
	Yes	28	68%
Policy made known	No	2	5%
	Yes	41	95%
Can relax policy	No	23	56%
	Yes	31	44%
Policy relaxed for staff research	No	6	38%
	Yes	10	63%
Policy relaxed for student research	No	5	31%
	Yes	11	69%
Policy relaxed for other reason	No	14	82%
	Yes	3	18%

Concerns about the value of software products to filter "inappropriate" material were noted in some of the participants' comments. For example, "Some of our schools have purchased software packages but these can restrict access to valuable information that is okay for use (word restrictive). It would be nice to have the Internet restrict access to certain websites by various usergroups (for a fee)." In addition, another respondent commented "We have not implemented a filtering software or excluded areas of Internet access. With hundreds of stations coming on-line, we may need to do so in future. We understand filtering software is far from ideal in limiting access."

One participant summed up his views on regulation by commenting "We do not feel we have a good handle on this challenging problem." The issue of content on the Internet was described in some comments:

- "Every school has policies concerning acceptable and non-acceptable behavior, conduct, and materials. These policies are media independent, for example, inappropriate material in electronic form has the same consequence as inappropriate material in print form."
- "Just as we select appropriate print resources, so do we select digital resources."
- "As a school district we are concerned with what is available on the Internet. There are many sites that have little or no educational value for students. We have developed an adopted District Policy which outlines our beliefs with cautions to staff, parents."
- "Access has been limited by availability. We have taken the position that we do not want the students visiting websites that have the content that we would not purchase in print versions (e.g., Playboy, Playgirl, neo-Nazi, etc.)"

Chapter IV

Discussion and Conclusions

This study investigated the issue of Internet crime, including its prevalence, and the feasibility of regulation, from the perspectives of police, university officials, and school officials. The intent of the study was to address the issue as presented in the introduction to this study. It is the author's belief that the obtained results contribute to the extension of knowledge on the issue of concern. The study provides information on the severity of the challenge associated with Internet crime. It also provides information that may be useful to educators, the legal community, and parents. Because research conducted on this topic is lacking, this study provides a good base on to which further studies could extend.

It appears that many people would like to see some regulation of the Internet implemented. In a Southam-Global Poll of adult Canadians conducted in 1997, 66% of the adults responded that they favored the government passing laws to regulate the Internet (Cobb, 1997). The difference in opinion concerns who should be responsible for this regulation. The majority of the participants in the study, including both academics and police officials, felt that regulation is not feasible, but most attempted to implement some degree of restricting access. This finding differs from that found by Burton (1995). However, quite similar findings were found in this study among the responses of police, school superintendents, and directors of computing centres at universities.

Summary of Findings

Police Questionnaires

It was a consensus that police departments found the issue of Internet crime as a big challenge, and one that is on the rise. Many police services across the country find themselves in need of adjusting to the demands resulting from this particular technological crime. A large majority of police participants suggested that fraud was the most prevalent of Internet crimes, and was investigated most often. The number of charges laid as a result of investigations ranged from 0-4 to 15+. Although most respondents indicated charges had been laid, the majority indicated that there had been no convictions related to these cases. Almost half of the police respondents indicated that they had never taken a proactive approach. The fact that there is some degree of proactive enforcement is somewhat surprising since Canada has typically been associated with reactive policing. It is also surprising as the limited staffing at most police departments makes proactive policing more difficult. The question did not take into account the type of enforcement (proactive or reactive) used most often. Most of the respondents indicated that they did not believe it was feasible to regulate the Internet. Many of the comments made regarding the issue of regulation concerned jurisdictional issues, since Internet crime has no geographical boundaries. Laws vary from country to country and are, therefore, difficult to enforce. The technical nature of the Internet was also conveyed as a difficulty impeding regulation because Internet sites are changing daily. A common theme inherent in the information gathered from police departments

concerned the need for worldwide political commitment. The police respondents felt that only when countries agree on common legislation can laws be effectively enforced.

University Questionnaire

It appears that most of the university officials surveyed see regulation of the Internet as something that should be done, and access to all users should be restricted. Policy restricting user access was most often developed by central administration and the groups affected were most likely not consulted. The consequences for a breach of the policy varied, with expulsion being the most extreme. A large majority of the respondents indicated success with the policy.

These results differed somewhat from those found by Burton (1995). Burton's findings indicated that a large majority of the respondents exercise no control over access to the Internet. Sixty-two of the university officials who completed Burton's survey indicated that there was no control of access exercised. According to the results of the present study, university officials in Canada appear to make their policies on controlling access more visible than the British universities surveyed in the Burton study. In the present study, 90% of respondents made their policies known, while in the Burton study, the policies were made known by 24% of the respondents. The respondents from the present study also indicated that they were more likely to relax the restrictions, if requested. Development of policy was also conducted by different groups in the two studies. In the Burton study, computer services was consulted most often, but in the present study, the policy was most likely developed after consultation with central

administration. Furthermore, seven respondents (21%) in the Burton study suggested that regulation of the Internet would be (or is) challenging.

There are also some differences in the findings of the present study and those found by Rasmussen et al. (1995), who surveyed American universities about their Internet policies. The public universities in the Rasmussen et al. study tended not to restrict access, mainly because they did not want to make moral decisions for their students. They found that their "proper use policies" were successful. The private institutions involved in the study also tended not to restrict Internet access. They relied on the "honor system" and on the students policing themselves. The students were also expected to adhere to "statements of student responsibilities" or "ethics of computing" waiver. This lack of controlling access at the public and private institutions varied from the Canadian universities surveyed in the present study, since most of the Canadian universities controlled access of students and staff. However, the fact that the American universities found their policies successful was a commonality with the present study.

School Questionnaire

Many of the school districts in Alberta saw the issue of regulation of the Internet as problematic, but are finding ways to adjust to the growing concerns. The majority of districts surveyed have implemented some control over all users. The issue of morality seemed to greatly affect the decision to control access. Most of the respondents indicated that a filtering program has been implemented in their district. The use of such a program was a major difference from the findings associated with universities. Acceptable use policies were frequently mentioned in the comments made by school

officials, and it appears that these user agreements may be becoming more prevalent. The consequences for breach of this policy varied, but the most common solution was students' loss of Internet privileges. Similar to the results of the university survey, the policy was deemed to be very successful.

Summary

Some degree of regulation was seen as necessary by the respondents of all three surveys. The differences regarding the amount of regulation at universities, as suggested by Burton (1995), Rasmussen (1995), and the present study, may be due to the timing of the studies. The Internet is much more popular now than it was in 1995, and institutions are adjusting to the new demands the Internet has provoked.

It may be suggested that school districts may be more rigid on the issue of restriction of access. The university results indicated no restrictions on access were placed on staff, the policy was more likely to be relaxed at universities than schools, and the size of the computer files was of greater concern than the moral or ethical nature of the files. The different reasons for control of access between universities and schools may be due to the age differences of the students attending these institutions. The moral nature of files may be seen as being more important than other reasons, such as the size of files, especially if the age of the user is considered.

Possible Solutions to Regulation

Myths about Accessibility of Obscene Material

The accessibility of obscene material on the Internet may be exaggerated. In most circumstances, a person has to search for this type of material. There are incidents when

a simple search uncovers some explicit webpages but, for the most part, a person must know what he/she is looking for and may choose links that have the potential to lead to obscenities. If you want to view adult content you can find it, in the same way that there are some individuals who will purchase adult magazines. Usually, the files that can be found most easily on the Internet can more easily be found in magazines and other printed literature. The chances of randomly stumbling across pornographic images are quite slim. One of the most prominent myths about the Internet is that pornography is quite prevalent. This myth may be largely due to the attention the media has given the topic. Pornography content actually constitutes a small portion of the Internet. In most cases, children would need to have some finely tuned computer skills to access some files, including the transformation of binary files into pictures (Elmer-Dewitt, 1995). Some of the files that contain explicit material are protected by passwords which need to be applied for, but sometimes there are no checks to ensure that the person making the application is of legal age. There may also be differences among various countries as to what is considered legal age to access pornographic material.

Filtering Products and Warning Labels

Popular filter products such as Net Nanny (1997) and CYBERsitter (1997) give parents and educators the ability to limit access by children to objectionable material on the Internet. CYBERsitter allows the computer owner to block words and phrases. Before the blocking occurs, the product examines the context in which the word or phrase is used. CYBERsitter can also alert parents and teachers if the user has attempted access into areas that were selected as restricted. The product claims to be impossible for

children to detect. Any site that focuses on such topics as adult or sexual issues, illegal activities, racism, or pornography are included in a list of objectionable sites, newsgroups, or chat lines provided by CYBERsitter.

Net Nanny's filtering lists are defined by the user, and parents and teachers can choose to block any words or phrases, sites, and content. It is also possible to limit access only to sites deemed suitable by the parents or teachers. Net Nanny can also prevent the loading of unauthorized CD-ROMs and other software. There is also a list provided of objectionable sites that can be downloaded from the Internet into the Net Nanny program. It should also be noted that the number of screening software products coming on the market is increasing in availability.

Although these filtering products can be effective in limiting access to some explicit material, they also have their drawbacks. For example, if certain words are blocked, valuable information may be lost. An example may be information on "sex education"; if the word sex is blocked, useful information in sex education may be limited. Because new sites are arriving on-line continuously, the lists of objectionable sites provided by most software programs may become outdated.

Warning labels or disclaimers do not limit the availability of explicit material, but they can allow users to be aware of the nature of the content of available Internet sites. If a disclaimer is present at the beginning page of a website, this gives the user the option either to view the site or to browse elsewhere. A disclaimer can also serve as a warning that only those users of legal age should be entering the sites. But again, it is possible that no measures are taken to verify the age of the user. Although the warnings may

pique the interest of the user, they place the onus on the user to make a "good" or "bad" choice. Internet providers may also choose to offer a disclaimer that objectionable material may be present on-line, or that content control is not regularly exercised. Once again, the responsibility of the provider is alleviated.

Warning labels or disclaimers may serve to be a viable option to make users aware that objectionable material exists on the Internet. Their usefulness is comparable to that of ratings or warnings present on television programs.

Self- Regulation and User Responsibility

Because of the aforementioned reasons, such as Internet sites changing daily, lack of time and resources, and the technical nature of the Internet, certain forms of regulation do not seem possible. Self-regulation and user responsibility seem to be the most feasible. What is needed most are responsible users, since service providers, law enforcers, and screening software are limited in the amount of restrictions they can employ. If computer users recognized the importance of moral values and put these to use, then they may be less likely to view obscene material or commit Internet crimes. In schools and universities, students should understand that they are responsible for their actions and need to make responsible choices. This would allow for a lot less controversy surrounding the Internet and could possibly decrease the amount and severity of Internet crimes.

Education of Users and the Legal Community

Education of users can be quite effective in changing the behaviors of computer users. If users are educated about the impact that their misconduct can have on other

users, they may be less likely to commit indecent acts. Information sessions regarding this topic can be helpful in schools, universities, and in workplaces.

The legal community also needs to be educated about potential areas of abuse on the Internet, as well as about the technical capabilities of computers and the Internet. This could facilitate the development of new Canadian legislation which needs to be adapted to coincide with the increase of Internet crimes. Education could also be useful to police who may be reluctant to face the challenge of new technology and to judges who may also be uneasy about computer technology.

Advice for Parents and Teachers

There are a number of safeguards parents and teachers can take to ensure that children do not become victimized by, or take part in, Internet crime. Most importantly, parents and teachers need to monitor the Internet activities of children in their care. Guardians also need to prevent children from spending much of their time browsing the Internet while working on computers. By keeping the household computer in a common area, or school computers in well supervised areas, the monitoring of computers could be much easier. It may be useful for parents and teachers to allow children to use the Internet through World Wide Web bookmarks previously selected by the guardian. If searches are to be conducted on-line, the guardian can provide the keywords that could be useful to find the information they are seeking. There are a number of tips that can be followed and warning signs to look for:

- Children should be told to not engage or respond to other users who send offensive email. Unfortunately email correspondence may develop into something the child is not prepared for.
- Children should report anything that they see as objectionable to the system operator, to parents, or teachers.
- Children should be told to never give out any personal information over the Internet.
- One-to-one meetings should never be set up with anyone a child meets on the Internet.
- Be aware of modems being used late at night. Children may be trying to keep their Internet activities hidden.
- Look for a child's use of new vocabulary that may be laden with heavy computer terms or sexual innuendoes.
- Be aware of credit cards and phone numbers being scanned into the computer.

For those parents and teachers who are not already familiar with computers, it is important that they at least learn the basics about computers and the Internet. The familiarity allows for more effective monitoring of activities.

Limitations of Study

There were a number of factors that limited the scope of this study. Firstly, the sample was limited by the small number of participants who completed the police and university questionnaires. The study likely would have been more representative if a larger number of participants had been recruited. In addition, the dichotomous responses provided by the questionnaires may have been better described through subsequent chi square analysis. The study would have been improved if a clearer distinction had been

made among such things as the Internet, newsgroups, chatgroups, and Bulletin Board Systems. In essence, the survey questions could have been refined.

Recommendations for Future Research

Further research is warranted in this subject area, especially since Internet crime is a growing concern. A more comprehensive study in which officials from various school districts in Canada are compared regarding their views on regulating use of the Internet. Useful information may also be gained by a comparison of the views of school officials at both the elementary and secondary levels. A number of other surveys into views on Internet regulation may also contribute further information to this subject area. A survey of Internet Service Providers and system operators regarding their views on regulation might provide some valuable insight. Another useful contribution might be to survey Internet users on their beliefs regarding regulation and the prevalence of Internet crime. A comparison of schools which have Internet access and those who do not could provide insight into the attitudes of students and teachers towards Internet crime. Views on prevalence of objectionable sites could also be determined via a comparison of those schools that regularly monitor sites, and those that do not. This could also be done by comparing those schools that limit students' access to the Internet through pre-selected bookmarks, for example, and those that do not. In addition, because pornography is given so much attention in the media compared to other Internet crimes, it may be useful to examine the issue of pornography on the Internet more closely to see just how prevalent it is. This could be determined through a survey of Internet sites or a more comprehensive survey of police departments than was done in the present study.

Conclusion

It appears that the most feasible solution to Internet regulation is that of user responsibility. Being aware that objectionable material exists on the Internet and exercising moral judgment are steps in the right direction. There is a need for the legal community to continue to adapt to the technological demands of Internet crime and for global officials to work towards common legislation solutions. There is also a need for parents and teachers to be aware of safeguards that can be taken towards making the Internet the valuable tool it is intended to be.

The present study has contributed to an area that has been largely neglected and provides a good basis on which future studies can build. Given that Internet crime can be called the crime of the future, further research on this topic is warranted. Undeniably, the debate concerning free speech and the issue of regulation will continue. Dealing with this modern crime may be one of the major challenges of the first decades of the twenty-first century.

References

Burton, P. F. (1995). Regulation and control of the internet: Is it feasible? Is it necessary?. Journal of Information Science, 21(6), 413-428.

Carey, P. (1996). Media law. Toronto: Carswell.

CNN. (1998, September 2). Fourteen nations join to bust huge Internet child porn ring. [On-line]. Available URL: http://cnn.com/WORLD/europe/9809/02/internet.porn.02/index.html

Cobb, C. (1997, December 23). Canadians want Internet regulations. New Glasgow Evening News, p. 8.

Coleman, G. (1996, August 25). Police chiefs target use of internet in crimes. Winnipeg Free Press, p. A7.

Cybercops: Angels on the net. (1996, January-February). Educom Review, 31(1), 34-38.

Cybersitter. (1997). Cybersitter: The most advanced internet filtering product available! [On-line]. Available URL: http://www.solidoak.com/cysitter.htm.

Diamond, E., & Bates, S. (1995). Law and order comes to cyberspace (and) Filtering the net. Technology Review, 98(7), 22-33.

Edmonton Police Services. Guide for parents, children and computers: The hidden danger. Edmonton, Alberta (brochure).

Elmer-Dewitt, P. (1995a, July 3). On a screen near you: Cyberporn. Time [On-line], 146(1). Available URL:

http://pathfinder.com/@@yEmoKwQA6LngpfCo/time/magazine/domestic/1995/950703.cover.html.

Elmer-Dewitt, P. (1995b, July 24). Firestorm on the computer nets. Time [On-line], 146(4). Available URL: http://pathfinder.com/@@WSdl4gQAbblEqEiA/time/magazine/domestic/1995/950724/950724.internet.html.

Frank, J. (1995). Preparing for the information highway: Information technology in Canadian households. [On-line]. Available URL: http://www.statcan.ca/english/SocTrends/infotech.htm.

Gibbs, W.W. (1997). Profile: Dan Farmer. Scientific American, 32-34.

Gold, M. (1996, October 3). Tracking cyberporn. Calgary Herald, p. H2.

Hanson, W. (1994). Student drivers on the information highway. Wilson Library Bulletin, 34-36, 132.

Hoffman, D.L., & Novak, T.P. (1997). Hoffman and Novak's critique of the Rimm study. [On-line]. Available URL: http://rhodes.www.media.mit.edu/people/rhodes/cyberpatrol/hn.on.rimm.html.

Hughes, S. (1996, June 1). Nova Scotians lured into internet scam. The Chronicle Herald Mail Star, p. C10.

Johnson, D.G. (1994). Computer Ethics (2nd ed.). In Crime, abuse, and hacker ethics. (1994). Educom Review, 29(5), 40-50.

Kurz, R.A. (1996). Internet and the law. Rockville, Md: Government Institutes Inc.

Laughon, S, & Hanson, W.R. (1996). Potholes on the infobahn: Hazardous conditions ahead? Multimedia Schools, 3(3), 14-23.

McCarten, J. (1996, July 13). Wider use of internet includes increased police intervention. Vancouver Sun, p. A5.

Morton, P. (1996, June 15-17). Net scams leave investors burned: Old-fashioned stock fraud thrives on high-tech internet. Financial Post, pp. 1,2.

Net Nanny. (1997). Net Nanny: The best way to protect your children and free speech on the net. [On-line]. Available URL: http://www.netnanny.com/nnfaq.html.

Organized criminals riding superhighway: Cops warned of internet porn. (1996, August 27). Montreal Gazette, p. A7.

Rasmussen, J.J, Williams, M., Peterson, B., Olson, J., Donaldson, C., & Feyder, A. (1997). Pornography on the internet. [On-line]. Available URL: http://www.gac.edu/~jrasmus3/research/table.html.

Reid, B. (1995). Critique of the Rimm study. [On-line]. Available URL: http://www2000.ogsm.vanderbilt.edu/novak/brian.reid.critique.html.

Rimm, M. (1995). Marketing pornography on the information superhighway. Georgetown Law Journal [On-line], 83(5), 1849-1915. Available URL: http://www.sics.se/~psm/kr9512-001.html.

Stephens, G. (1995). Crime in cyberspace. The Futurist, 29, 24-28.

Torgerson, C. (1997). Potholes on the information highway: An elementary educator's perspective. Unpublished manuscript, University of Alberta.

Treese, W. (1994). The internet index. [On-line]. Available URL: http://www.openmarket.com/info/internet-index/current.html.

Wallace, J.D., & Mangan, M. (1996). Sex, laws, and cyberspace: Freedom and regulation on the frontiers of the online revolution. Markham, Ontario: Fitzhenry & Whiteside Ltd.

Wolynski, J. (1995). Obscene communications on the net. Information Technology Security Bulletin [On-line], 40. Available URL: http://www.rcmp-grc.gc.ca/html/bull40-e.htm.

Appendix A - School Questionnaire

Please read the following questions carefully, and choose the appropriate response. The required time to complete the questionnaire is approximately 20 minutes.

Please state your title _____

1. Does your school district restrict or prevent access to any sites on the internet, or particular newsgroups?

___ No control of access exercised. Please go to question 10.
___Some access by students controlled
___Some access by staff controlled
___Some access by all users controlled

2. Here are some possible reasons for controlling access to certain internet sites and newsgroups:

a. concern over legal action under obscenity laws
b. concern over legal action under race relation laws
c. concern over legal action under sexual harassment laws
d. concerns about the moral, ethical, religious or other nature of the files
e. concern over the size of the files

Please list any files, sites. etc. to which you control access and why you do so, using the letters above (e.g. alt.binaries *)

3. Have you purchased a program for limited use?

Yes ___ No ___

4. Is the policy on controlling access made known (in print or electronically) to other users?

Yes ___ No ___

5a. Can this policy be relaxed under certain circumstances?

Yes ___ No ___

b. If yes, what are the circumstances?

___ Necessary for staff research
___ Necessary for student research
___ Other (please specify) _____

6. How was this policy arrived at?

___ Decision by central administration
___ Decision by computer consultants
___ Decision by other body or group (please specify) _____

7. Was there any consultation with the group(s) affected?

Yes ___ No ___

8. Has the policy been successful?

Yes ___ No ___

9. What are the consequences for breach of policy?

10. Any further comments or observations on the control of access to internet resources?

Thank you for your time.

Please return completed questionnaire to: **Lisa Clyburn**
310, 10711- Saskatchewan Dr.
Edmonton, AB
T6E 4S4

A postage-paid envelope is provided.

Appendix B - University Questionnaire

Please read the following questions carefully, and choose the appropriate response. The required time to complete the questionnaire is approximately 20 minutes.

Please state your title _____

1. Does your institution restrict or prevent access to any sites on the internet, or particular newsgroups?

___No control of access exercised . Please go to question 10.
___Some access by students controlled
___Some access by staff controlled
___Some access by all users controlled

2. Here are some possible reasons for controlling access to certain internet sites and newsgroups:

a. concern over legal action under obscenity laws
b. concern over legal action under race relation laws
c. concern over legal action under sexual harassment laws
d. concerns about the moral, ethical, religious or other nature of the files
e. concern over the size of the files

Please list any files, sites. etc. to which you control access and why you do so, using the letters above (e.g. alt.binaries *)

3. Have you purchased a program for limited use?

Yes ___ No ___

4. Is the policy on controlling access made known (in print or electronically) to other users?

Yes ___ No ___

5a. Can this policy be relaxed under certain circumstances?

Yes ___ No ___

b. If yes, what are the circumstances?

___ Necessary for staff research
___ Necessary for student research
___ Other (please specify) _____

6. How was this policy arrived at?

___ Decision by central administration
___ Decision by computer services
___ Decision by other body or group (please specify) _____

7. Was there any consultation with the group(s) affected?

Yes ___ No ___

8. Has the policy been successful?

Yes ___ No ___

9. What are the consequences for breach of policy?

10. Any further comments or observations on the control of access to internet resources?

Thank you for your time.

Please return completed questionnaire to: **Lisa Clyburn**
310, 10711 - Saskatchewan Dr.,
Edmonton, AB
T6E 4S4

A postage-paid envelope is provided.

Appendix C - Police Questionnaire

Please read the following questions and check the appropriate response. The required time to complete the questionnaire is approximately 15 minutes.

1. How many charges have been laid as a result of investigations your division has been involved in?
   - ___ 0-4
   - ___ 5-9
   - ___ 10-14
   - ___ 15+

2. Have there been any convictions?
   ___ Yes ___ No If Yes, how many? ___

3. What internet crime do you see as being most prevalent?
   - ___ Fraud
   - ___ Child Pornography
   - ___ Distribution of pornography
   - ___ Defamation
   - ___ Copyright infringement
   - ___ Other (please specify) _____

4. What crime is most often investigated within your division?
   - ___ Fraud
   - ___ Child pornography
   - ___ Distribution of pornography
   - ___ Defamation
   - ___ Copyright infringement
   - ___ Other (please specify) _____

5. How many complaints are you currently investigating?
   - ___ 0-4
   - ___ 5-9
   - ___ 10-14
   - ___ 15+

6. In regards to the investigation of internet crime, have you ever taken a pro-active approach, as opposed to a reactive one?

___ Yes ___ No

7. Do you think it is feasible or possible to regulate the internet?

___ Yes ___ No

8. Could you comment on how you believe the internet could be regulated?

9. Any further comments on the issue of internet crimes?

10. Any further comments on the issue of regulating the internet?

Thank you for your time.

Please send completed questionnaire to: **Lisa Clyburn**
310, 10711 - Saskatchewan Dr.,
Edmonton, AB
T6E 4S4

A postage-paid envelope is provided.

Appendix D - Universities Used in Study

University Addresses

Computer and Network Services
302 General Services Building
University of Alberta
Edmonton, AB
T6G 2E1

Security Administration
University Computing Services
University of British Columbia
6356 Agricultiral Road
Vancouver, BC
V6T 1Z2

Academic Computing and Networking
U of Manitoba
Winnipeg, MB
R3T 2N1

Director
Department of Computing Services
56 Physics
U of Saskatchewan
Saskatoon, SK
S7N 0W0

Director
Computing and Network Services
4 Bancroft Ave and 255 Huron St.
U of Toronto
Toronto, ON
M5S 1A1

Director of Computing and
Telecommunications
McGill Computing Centre
805 Sherbrooke St. W.
Montreal, PQ
H3A 2K6

Director
Computing Services
P.O. Box 4400
Fredericton, NB
E3B 5A3

Director of Academic Computing
Services
Dalhousie University
Computer Centre, Killam Library
6225 University Ave.
Halifax, NS
B3H 4H8

Director
Computer Services
Atlantic Veterinary College Building
UPEI
550 University Ave.
Charlottetown, PE
C1A 4P3

Director
Dept. of Computing and
Communications
Memorial University
St. John's. Nf
A1C 5S7

Director
Information Systems and Technology
U of Waterloo
Math and Computer Building
Room 1052
Waterloo, ON
N2L 3G1

Director
Computing and Communications
35 University Private
Thompson Hall, Room OSOA
University of Ottawa
Ottawa, ON
K1N 6N5

Director
Information Technology Services
Natural Science Centre, Room 244
University of Western Ontario
London, ON
N6A 5B8

Director
Computing Services
LB-800 1400 de Maissoneuve W.
Concordia University
Montreal, PQ
H3G 1M8

Appendix E - Letter of Explanation

Dear Sir or Madam:

As a researcher and graduate student at the University of Alberta, I am currently engaged in a study investigating criminal activities on the Internet, and viewpoints concerning the issue of whether or not the Internet should be regulated. I am interested in issues such as: What policies are implemented by universities and schools to control access to obscenities on the Internet? What methods can teachers and parents employ to prevent such access? How prevalent are investigations by police into Internet crimes?

The information gained from this project will likely contribute to the awareness of criminal activity on the Internet, and provide further insight into the debate concerning regulation of the Internet. It may also provide valuable information to parents and teachers responsible for the guidance of children browsing the Internet. The items on the questionnaire deal with existing policies at your institution and your enforcement of these policies. Completing the questionnaire should require 20 minutes or less.

This study has been approved by the Ethics Review Committee of the Department of Educational Psychology, University of Alberta. Your responses to the questionnaire will be kept confidential, and your participation is entirely voluntary. The completion of the questionnaire signifies your consent to participate in the study.

Your response is very important to the success of this study. We very much appreciate your completing and returning the questionnaire as soon as possible in the enclosed, postage-paid envelope.

If you would like further information about the project, please call Lisa at (519)884-3306.

Thank you for your consideration.

Sincerely,

Lisa Clyburn
M.Ed. Candidate

E.W. Romaniuk, PhD
Thesis Supervisor

Appendix F - Follow-up Letter Sent with All Surveys

Dear Sir or Madam:

The enclosed survey instrument is concerned with possible crimes on the Internet and the feasibility of regulating the Internet. It is part of a continuing study conducted at the University of Alberta for a masters thesis. The project is concerned specifically with such issues as: What policies are implemented by universities and schools to control access to obscenities on the Internet? What methods can teachers and parents employ to prevent such access? How prevalent are investigations by police into Internet crimes?

Although I know you are extremely busy, I am re-sending you this survey and asking for your cooperation in completing the survey. If you have already returned the first survey, thank you for your time and cooperation, and disregard this letter. If you have not returned the first questionnaire, your response to this questionnaire is very important to the success of this study. The information gained from this project will hopefully contribute to an awareness of criminal activity on the Internet, and provide further insight into the debate concerning attempts to regulate the Internet. It may also provide valuable information to parents and teachers in guiding children who are browsing the Internet. The time required to complete the questionnaire is about 15 minutes or less.

Your participation in this research project is entirely voluntary. All your responses to the questionnaire will be kept confidential. Completion of the questionnaire signifies your consent to participate in the study.

We very much appreciate your completing and returning the questionnaire as soon as possible in the enclosed, postage-paid envelope..

If you would like further information about the project, please call Lisa at (403)434-9484. E-mail: lclyburn@gpu.srv.ualberta.ca

Thank you for your consideration.

Sincerely,

Lisa Clyburn
M.Ed. Candidate

E.W. Romaniuk, PhD
Thesis Supervisor

Appendix G - List of Police Agencies Used in Study

Police Addresses

Ottawa Police
Federal Services Directorate
Economic Crime Branch
Technological Crime Section
Room H-555, 1200 Vanier Parkway
Ottawa, ON
K1A 0K2

Calgary Police Services
133 6 Ave. SE
Calgary, AB
T2G 4Z1

Edmonton Police Services
9620 - 103A Avenue
Edmonton, AB
T5H 0H7

Winnipeg Police Services
P.O. Box 1680
Winnipeg, MB
R3C 2Z7

Toronto Police Services
40 College St.
Toronto, ON
M5G 2J3

Halifax Police
21 Mount Hope Ave.
Dartmouth, N.S.
B2V 3Z3

Vancouver Police Services
312 Main St.

Vancouver, BC
V6A 2T2

Montreal RCMP
4225 Dorchester Blvd. W.
Montreal, PQ
H3Z 1V5

RCMP
P.O. Box 9700
Station B
St. John's, Nf.
A1A 3T5

RCMP
1721 8th St.
East Saskatoon, SK
S7H 0T4

Quebec Centrale de Police
275 Gignac St.
Quebec, PQ
G1K 2L3

Saint John Police Force
Computer Unit
P.O. Box 1971
St. John, NB
E2L 4L1

RCMP
450 University Ave.
Charlottetown, PE
C1A 4P1

Regina Police Services
1717 Osler St.
Regina, Sk
S4P 3W3

Appendix H – List of School Districts Used in Study

Aspen View Regional Division No. 19
Battle River Regional Division No. 31
Black Gold Regional Division No. 18
Buffalo Trail Regional Division No. 28
Calgary Roman Catholic Separate School District No. 1
Calgary School District No. 19
Canadian Rockies Regional Division No. 12
Chinook's Edge Regional Division No. 5
Christ the Redeemer Catholic Separate Regional Division No. 3
Clearview Regional Division No. 24
East Central Alberta Catholic Separate Schools Regional Division No. 16
East Central Francophone Education Region No. 3
Edmonton Catholic Regional Division No. 40
Edmonton School District No. 7
Elk Island Public Schools Regional Division No. 14
Evergreen Catholic Separate Regional Division No. 2
Foothills School Division No. 38
Fort McMurray Roman Catholic Separate School District No. 32
Fort McMurray School District No. 2833
Fort Saskatchewan Roman Catholic Separate School District No. 104
Fort Vermillion School Division No. 52
Golden Hills Regional Division No. 15
Grande Prairie Roman Catholic Separate School District No. 28
Grande Prairie School District No. 2357
Grande Yellowhead Regional Division No. 35
Grasslands Regional Division No. 6
Greater St. Albert Catholic Regional Division No. 29
High Prairie School Division No. 48
Holy Spirit Roman Catholic Separate Regional Division No. 4
Holy Trinity Roman Catholic Regional Division No. 36
Horizon School Division No. 67
Lakeland Roman Catholic Separate School District No. 150
Lethbridge School District No. 51
Livingstone Range School Division No. 68
Lloydminister Public School Division
Medicine Hat School District No. 76
Medicine Hat Catholic Separate Regional Division No. 20
North Central Francophone Education Region No. 4
Northeast Francophone Education Region No. 2
Northern Gateway Regional Division No. 10
Northern Lights School Division No. 69
Northland School Division No. 61
Northwest Francophone Education Region No. 1

Palliser Regional Division No. 26
Parkland School Division No. 70
Peace River School Division No. 10
Peace Wapiti Regional Division No. 33
Pembina Hills Regional Division No. 7
Prairie Land Regional Division No. 25
Prairie Rose Regional Division No. 8
Red Deer Catholic Regional Division No. 39
Red Deer School District No. 104
Rocky View School Division
Sherwood Park Catholic Separate School District No. 105
South Central Francophone Education Region No. 6
Southern Francophone Education Region No. 7
St. Albert Protestant Separate School District No. 6
St. Paul Education Regional Division No. 1
St. Thomas Aquinas Roman Catholic Separate Regional Division No. 38
Sturgeon School Division No. 24
Sundance Catholic Separate Regional Division No. 10
Westwind Regional Division No. 9
Wetaskiwin Regional Division No. 11
Wild Rose School Division No. 66
Wolf Creek Regional Division No. 32